Controlled Use of Excess Backbone Bandwidth for Providing New Services in IP-over-WDM Networks

A.Nucci[1], N.Taft[2], Chadi Barakat[3], Patrick Thiran[4]

[1] – Sprint Advanced Technology Labs, Burlingame CA, USA

[2] – Intel Research Berkeley, Berkeley CA, USA

[3] – INRIA, 06902 Sophia Antipolis, France

[4] – LCA-ISC-I & C, EPFL, CH-1015 Lausanne, Switzerland

Abstract

In this paper we study an approach to Quality of Service that offers end-users the choice between two classes of service defined according to their level of transmission protection. The first class of service, called *Fully Protected* (FP), offers end-users a guarantee of survivability in the case of a single link failure; all FP traffic is protected using a 1:1 protection scheme at the WDM layer. The second class of service, called *Best-Effort Protected* (BEP), is not protected; instead restoration at the IP layer is provided. The FP service class mimics what Internet users receive today. The BEP traffic is designed to run over the large amounts of unused bandwidth that exist in today's Internet. The motivation of this approach is to give carriers a mechanism for increasing the load carried on backbone networks without reducing the QoS received by existing customers. In order to support two such services, we have to solve two problems: the off-line problem of mapping logical links to pairs of disjoint fiber paths, and an on-line scheduling problem for differentiating packets from two classes at the IP layer. We provide an *Integer Linear Programming* model [1] and an algorithm based on a *Tabu Search* meta-heuristic to solve the mapping problem, and a simple but efficient scheduler based on *Weighted Fair Queuing* for service differentiation at the IP layer. We consider numerous requirements that carriers face and illustrate the tradeoffs they induce. We evaluate the throughput, delay and loss performance of the two traffic classes and illustrate that we can successfully increase the total network load by a factor between three and ten and still meet all the carrier requirements.

I. Introduction

The Internet backbone contains a large amount of capacity that is currently not being used. Carriers today are very interested in carrying additional load on their networks in order to generate additional revenue; however they are concerned about not reducing the quality of service received by existing customers. The three main reasons why the Internet contains unused capacity are because of *equipment redundancy*, *overprovisioning*, and *the link ugrade process*. Equipment redundancy typically leads to a multiplicity of links and/or

This work was done when Nina Taft was at Sprint ATL; she is currently affiliated with Intel Research Berkeley, CA.

[1]The Integer Linear Programming Model (ILP) is presented in the Appendix and is included for review purpose only.

nodes. Overprovisioning usually implies that network links are run at low utilization levels. Redundancy of equipment and overprovisioning are used to protect the backbone against failures. Some recent research studies have started to uncover the nature and extent of failures in today's IP backbones [2], [3]; these findings have revealed that failures of one type or another occur almost on a daily basis [2], and roughly 12% of failures are related to optical layer failures [3]. With technologies such as WDM, a single fiber failure can bring down a large number of IP paths. Most large carrier networks today use highly meshed topologies to prevent network partitioning in the event of widespread failures involving multiple links.

Upgrading the links (e.g., converting an OC-48 to an OC-192 link) in a large backbone is a time consuming process. For example, upgrading a single large inter-POP backbone link can take a few months, while upgrading a sizeable portion of the entire network can take over a year. Each time a link is upgraded, a "pocket" of additional bandwidth becomes available. But this is not really available to users because (1) for some users the shortest paths they use may not traverse the new fast link, (2) for other users the sequence of links their packets follow may traverse the new link, but the other links in the sequence will be older slower ones and these slower links determine the end-to-end throughput, and (3) if the upgraded link is in the main working path, it may not be used if the backup path has not also been upgraded at the same time. When a network is partially upgraded, and has many pockets of bandwidth scattered over the topology, a potentially large number of users could indeed profit from this new capacity, if it is properly managed.

In this paper we propose that carriers provide two classes of service, one of which would mimic today's service and a second one that would provide a lower quality of service. The idea is for the lower-grade service to be carried on the "excess" bandwidth in the backbone in such a way that has no impact on the Service Level Agreements (SLAs) promised to the higher-grade service. The majority of time this excess bandwidth is unused, hence the lower-grade service will experience good performance and can support a good SLA. When this excess bandwidth becomes needed in a failure scenario, we drop as many packets as necessary from the lower-grade service in order to ensure there is enough bandwidth to protect the higher-grade service.

In order to achieve this, the two classes of service should be differentiated by their *level of protection* against failures and the packets needed to be marked according to the their class of service. The first class, called *Fully Protected* (FP), offers users the insurance that they will not suffer service interruption in the case of a single failure. Protection is provided at the WDM layer via a 1:1 protection scheme that guarantees fast recovery after a single failure. The second class of service, called *Best Effort Protected* (BEP) is new. It does not provide a specific guarantee on service disruption. Instead, in the case of failure, it offers to restore

as much of the affected traffic as possible. For a survey on protection and restoration strategies see e.g., [13].

Recently the problem of service management has gained a lot of attention in the optical community ([5], [14], [16], [15], [17], [9]). Proposals for different service classes in optical networks are introduced in Gerstel and Ramaswami [14]. Ramamurthy and Mukherjee [15] study the traditional 1+1 and 1:1 protection strategies at the WDM layer for a single class of traffic. They formulate the corresponding Integer Linear Program (ILP) optimization problem applicable to small networks. Mohan and Somani [16] propose a class of service that offers a minimal level of protection to every connection. They claim that if the demands are highly dynamic, it is possible to select routes whose (shared) back-up paths have a specified maximal non-zero probability of being unavailable if a failure occurs. Sridharan and Somani [17] formulate the ILP problem when three different service classes co-exist. They try to minimize the capacity requested by all working and backup paths, weighted by the traffic class to which it belongs (since each class brings in a different amount of revenue). Ramamurthy and Mukherjee [15] prove that the general problem is NP-complete for a single class of traffic. Hence the recent proposal for three classes of traffic at the WDM layer may be too complex to apply to real networks.

In an IP/WDM network, survivability can be provided at the IP layer or at the WDM layer. Each layer presents different advantages and drawbacks [8], [4]. Some multi-layer protection/restoration schemes can adequately combine the advantages of each layer and still avoid most of their disavantages [7]. They raise another challenge however, namely the complexity of coordinating the different restoration schemes at the various layers (some solutions are proposed in [7]). In this paper, this race between the layers for restoring traffic is circumvented by allocating this task to a different layer for each traffic class. FP traffic is rapidly and completely protected at the WDM layer, whereas BEP traffic is restored (at a slower scale) at the IP layer.

In [18] we initially presented the idea of two classes of service differentiated by their level of protection and we have shown that networks can safely carry a much larger load (in scenarios without failures) if they support these two service classes. In that work, we proposed an ILP model to find the primary and backup paths (sequence of fibers in the physical topology) for each logical link and to maximize the BEP traffic carried by the network in the no failure scenario. This problem is known in literature as a **mapping problem**. We did not study the restoration of the BEP traffic after the occurrence of a physical link failure. This is an important issue because it is clearly preferable for BEP traffic to experience a smooth, gradual degradation rather than a sudden, total disruption during failure episodes. By considering single failure events in our

solutions we can reduce the likelihood of total disruption and instead push the solutions towards ones that will yield smooth degradations. In this paper, we thus extend our work by incorporating the impact of single failure events. We incorporate additional constraints that carriers face, consider fairness in the excess bandwidth repartition, and provide a heuristic solution based on Tabu Search methodology that can scale to large networks. In order to provide a complete solution to supporting our two proposed services, we also **design a scheduler** that is needed at the IP layer to distinguish packets from the two services during failure episodes. The scheduler is based on *Weighted Fair Queueing* mechanism and it is transparent to both classes when the network is in normal operation (i.e., no failures). Our scheduler helps ensure that FP packets continue to experience the same SLA after failures, while BEP packets may experience a degradation. An appealing advantage of our scheduler is that it does not require any particuler signaling to switch between the no-failure and failure mode, and this switching is driven by the change in the available bandwidth at the WDM layer. The heuristic algorithm and scheduler also constitute extensions to our earlier work.

The goals of this paper are: i) to quantify how much BEP traffic can be carried on the network without impacting the FP service; ii) to determine how to allocate the BEP traffic load among all the logical connections such the partition of the BEP traffic is as fair as possible; iii) to maximize network-wide load carried while simultaneously balancing the tradeoffs of designing for normal operating conditions versus for failure modes; iv) to assess the service degradation during failure episodes; and v) to evaluate the success of the composite mapping and scheduling solutions by examining the performance of each class of service in terms of throughput, delay and losses at the IP layer. Task (v) is carried out using *ns* simulation. The output of the mapping problem solution is used to establish the physical and logical topologies, that are in turn used as inputs to the simulator.

The remainder of this paper is organized as follows. The FP and BEP classes of service are fully defined in Section II. In Section III we explain which components of the overall problem belong to which layer (physical or logical), give a formal problem statement and describe our approach. A heuristic solution based on Tabu Search methodology is introduced in Section IV while our optimal ILP solution is provided in the Appendix. The scheduler is described in Section V. Performance results for both medium-sized and large networks are presented and discussed in Section VI, along with a validation of our heuristic. Section **??** concludes the paper.

II. Definition and Provisioning of Classes of Service

The **Fully Protected (FP)** service guarantees its customers that their traffic is protected against any single point of failure in the backbone. FP traffic is protected via pre-computed, dedicated backup paths at the

WDM layer, using a 1:1 protection strategy. Failures are transparent to the IP layer for this class of traffic. In a 1:1 protection scheme, the FP traffic is transmitted only on one path (called the *working* or *primary* path). If this path fails, the sender and receiver both switch to the other path (called the *backup* path). Our idea is to take advantage of 1:1 protection because the reserved but unused capacity on the backup path can be given to unprotected traffic whose packets would be dropped in the case of a failure.

The **Best Effort Protected (BEP)** service is one whose traffic runs on the excess backbone capacity during *normal* operation (i.e., a network state with no failures). The BEP traffic of each logical connection can be routed on either the primary or the backup path, but not on both (i.e., it cannot be split over two paths). When a failure occurs, the available bandwidth drops on all logical links that share this fiber. Our IP scheduler enters into action and discards the BEP packets as needed while protecting the FP packets. Thus the SLA performance, in terms of packet drop rate, received by the BEP traffic depends upon the amount of overprovisioning that exists after both FP and BEP traffic have been accomodated.

We point out that in an environment in which each logical connection is protected via a 1:1 scheme at the WDM layer, and in which failures happen one at a time, the logical topology will always be connected. Thus the logical topology will be always able to apply a restoration strategy at the IP layer, and does not suffer from the *failure propagation* problem described in [20], [21], [22].

III. Mapping: Problem Statement

The main problem we address is to find a mapping of IP-layer logical links to physical fibers such that (1) the FP traffic, specified by an FP traffic matrix, is protected, and (2) we maximize network-wide load (including both traffic classes) subject to a constraint imposing a fairness policy on the allocation of BEP load among all the logical connections. Our intent is to add BEP traffic into the system such that there is no impact at all on the protection quality received by the FP traffic in the case of either a single failure or even multiple failures as long as none of them is a *critical* failure. In this context, a *critical failure* is a multiple failure scenario that brings down a set of links such that both the working and backup paths of the same logical link are interrupted.

We focus on PoP-to-PoP (Point-of-Presence) topologies at the IP layer, rather than on router-to-router topologies that consist of hundreds of routers. A PoP is an ensemble of core and access routers that usually reside in a single building in a metropolitan area. PoPs are interconnected via inter-PoP links attached to the core routers. The access routers are used to connect customers to the backbone. With this topology, the logical links we map capture the inter-PoP backbone links. Access routers can be ignored because they do not connect directly to other PoPs or other routers in the backbone.

The block diagram in Figure 1 clarifies the inputs and outputs of the mapping problem. A number of inputs to our problem, which define requirements and constraints, come from the IP layer (labeled "network inputs" in the figure). Two of the features we support, fairness and the topology tradeoff parameter (explained below), would be specified by an operator as they essentially define policies (hence labeled as "policy inputs" in the diagram). We next discuss each of the elements in this diagram and try to clarify which components of the problem are related to the logical (IP) layer and which are part of the physical (WDM) layer. To be clear, we state some definitions of basic terms. We use the expression *logical link* to refer to a single link between two PoPs at the IP layer. We use the term *logical connection* to refer to a sequence of logical links. Each logical link corresponds to a sequence of one or more physical links interconnected via optical cross-connects (OXCs).

The **FP traffic matrix** is a part of the logical layer. We decided to focus on maximizing the amount of BEP traffic carried while letting the FP traffic be specified by an input demand matrix. The reason for this is because capacity planning in the Internet is typically done using an IP layer traffic matrix that specifies the average amount of bandwidth that needs to flow between any two PoPs or PoPs in a domain. After we choose an initial matrix, we scale the entire matrix up, in order to load the maximum amount of FP onto our network. By "scaling up" we mean that we multiply all elements in the matrix by a constant factor that is as large as possible. The limit on how much the matrix can be scaled up is defined by the maximum amount we can protect.

The **IP routes** are those given by either the OSPF or IS-IS protocol that operates at the IP layer. These protocols usually compute shortest-path routes between PoPs. A path specified by OSPF (or IS-IS) is thus a sequence of *logical links*.

Both the FP traffic matrix and the IP routes are inputs to our problem. Using these two inputs, together with the logical topology we can calculate the aggregate load for each logical link by routing the *FP traffic matrix* over the *logical topology* according to the OSPF *IP routes*. As depicted in the block diagram, this is considered as a preprocessing step to the optimization problem. Three of these things - the FP traffic matrix, the IP routes, and the logical link FP load (all coming from the IP layer) - constitute the network inputs needed for our optimization problem at the physical layer.

The optimization procedure needs to find a pair of disjoint fiber paths for each logical link. One fiber path is for the working path and the second is for the backup path. There are typically a large number of such possible pairs for each logical link. We choose among the many candidate solutions by evaluating the corresponding amount of BEP traffic that maximizes our objective function after we have satisfied the demands for FP traffic. Since each logical connection is allowed to carry a certain amount of BEP traffic,

the network-wide view of the total BEP traffic carried can also be expressed as a **BEP traffic matrix** with the same rows and columns as the FP traffic matrix.

We should mention at this point that we cannot solve the mapping problem separately for the FP and BEP traffic. Indeed the BEP traffic takes the same routes as the FP traffic at the logical layer, and is mapped on the working or back-up path of the logical link for the FP traffic at the physical layer. The two traffic classes need therefore to be considered simultaneously in the mapping problem. In particular, we cannot consider the FP traffic matrix as a simple "bias" on the capacity of the logical links available for BEP traffic.

We now explain our objective function more carefully. We want to select a mapping that is good under two types of scenarios: the normal network state in which no link has failed, and the network state in which a single link has failed. If the optical layer is composed of L physical links, then the number of failure scenarios is L. The network, or topology, for each of the L failure scenarios, is the original topology with one link missing. Since we want to consider L single failure scenarios (we also used the term "failure modes") and 1 normal scenario with no failures, we essentially need to do an optimization over $L+1$ images of the backbone topology.

A mapping that considers the no failure mode only could assign a large amount of the spare capacity to BEP traffic. Since the BEP traffic is completely unprotected at the WDM layer, this could produce very bad performance, in terms of BEP traffic lost, when some physical links fail. Thus by focusing on the no failure mode alone, we would be able to carry a large amount of BEP traffic but experience potentially very poor performance during failures. By considering the failure modes, we can mitigate the performance degradation at the time of failures. A mapping that considers only failure modes would encourage the use of small amounts of BEP traffic as it would only load up an amount of BEP that could survive the particular failure. We thus define a *topology tradeoff parameter*, called W with $W \in [0, 1]$, that balances the amount of emphasis put on the normal topology versus those (with a link missing) that represent failure modes.

Our objective function contains two terms; the first term specifies the amount of BEP traffic carried by the network in the normal operating state (i.e., no-failure-mode), while the second one is the BEP load still carried by the network after the occurrence of a single failure, and averaged over all the possible single failures. We state this more formally as follows. Let $d_{S_0}^{kh}(BEP)$ denote the BEP traffic carried by the connection $(k, h) \in \mathcal{C}$ in the no failure mode (denoted by S_0), where $\mathcal{C}$ denotes the set of all logical connections flowing at the IP layer. Let $d_{S_{mn}}^{kh}(BEP)$ denote the BEP traffic carried by the connection $(k, h) \in \mathcal{C}$ when fiber (m, n) has been involved in a failure. The notation S_{mn} refers to the failure mode for link (m, n), i.e., it indicates a network state in which the physical topology is missing link (m, n). Let E^0 denote the set of edges in the optical layer topology (graph) and thus $(m, n) \in E^0$. Our objective function $\mathcal{F}$ is now given by

$$\mathcal{F} = (1 - W) \sum_{(k,h) \in \mathcal{C}} d^{kh}_{S_0}(BEP) + \frac{W}{|S_{mn}|} \sum_{(k,h) \in \mathcal{C}, (m,n) \in E^0} d^{kh}_{S_{mn}}(BEP). \quad (1)$$

Note that by modifying the weight W, we are able to reach solutions with different characteristics. When more importance is given to the first term (smaller W), more BEP is carried in the no failure mode but the average amount of BEP lost is larger when failures occur. On the other hand, if more importance is given to the second term (larger W), less BEP traffic is lost during the failures but less BEP traffic is carried by the network during normal conditions. The topology tradeoff parameter W could be chosen as a function of the probability of a link failure. If the link failure probability is very low, then clearly we want a small W so that the topology under normal operating conditions is given a very large weight. Conversely if the probability of failure is high, more importance should be given to the failure modes.

There are a multitude of ways in which BEP can be added to the spare capacity because there are many combinations of bandwidth that can be given to each connection, and each connection can route its BEP traffic on either the working or backup paths. Our ILP considers all possible strategies for adding BEP traffic and uses the objective function $\mathcal{F}$ as the criterion for selecting the best solution. While this achieves the objective, our experience shows us that this approach tends to lead to a very unbalanced distribution of the BEP load - giving large amounts of traffic to some connections and close to zero to others. In particular, single hop connections tend to receive a large amount of BEP while longer multihop connections receive very little. We believe that carriers would find this unappealing because of the unfairness. For that reason we include in our problem the concept of a **fairness policy**. We present two different fairness policies to allocate the BEP bandwidth among all the logical connections. The first policy is called **Minimum Guaranteed fairness policy (MinG)**. According to this policy, each logical connection must receive a minimum bandwidth for its BEP traffic, denoted as Z_{min}. After having met this even distribution, there is no further fairness mechanism implemented and each logical connection is free to get as much as it can. This policy is a first step towards the second policy presented, called **Maximum-Minimum fairness policy (MaxMin)**. This policy forces each logical connection sharing a bottleneck logical link to receive the same share of the bandwidth left for BEP traffic. Note that the second policy introduces more fairness among all the logical connections. We will show that the more fairly the BEP bandwidth is distributed, the less BEP load the network will be able to carry.

We now give the formal problem statement, incorporating all of the elements above.

GIVEN:

i) a physical topology (which must be at least biconnected), whose nodes are optical cross connects (OXCs)

interconnected by optical fibers that support a limited number of wavelengths and have limited capacity;
ii) a logical topology whose nodes are IP PoPs interconnected by logical links. These links have a finite limit on the total amount of traffic they can carry (including both FP and BEP). The limit comes from the capacity of their line cards;
iii) an FP traffic matrix, denoted $D_{FP} = [d^{kh}(FP)] \geq 0$, that defines the FP traffic demand for each pair of PoPs (k, h) at the IP layer. We call these pair origin-destination (OD) pairs;
iv) the routing paths selected at the IP layer for each OD pair of PoPs. This set of routes is denoted by $\mathcal{R}$;
v) a 1:1 FP protection strategy at the WDM layer;
vi) a fairness policy to allocate BEP traffic among all the logical connections;
vii) the objective function F defined above;

FIND

Primary and backup paths for each logical link and the BEP traffic matrix $D_{BEP} = [d^{kh}(BEP)] \geq 0$ for each pair of PoPs (k, h) at the IP layer in the regular condition in such a way that the network is able to:
i) carry the amount of FP traffic defined as an input by the FP traffic matrix D_{FP}.
ii) the objective function F is maximized.

IV. Solution to Mapping Problem

We develop two solutions to this problem. This first one uses optimization techniques to find an optimal solution based on formulating the problem as an Integer Linear Program (ILP). Although this approach can find optimal solutions, it is limited in its applicability since even for moderate size networks, obtaining an optimal solution to this problem becomes quite cumbersome due to the large number of variables and constraints involved in its formulation. Indeed, a simpler version of this problem, in which one tries to optimize the network load for only one class of service, was already proven to be NP-complete [15]. US backbone carriers can have upwards of 30 OXCs and 50 fibers in a physical topology, and upwards of 20 PoPs and 40 bidirectional logical links at the IP layer. It is thus clear that heuristic solutions are the only practical candidate solutions that carriers can consider using. Our second solution defines a heuristic algorithm based on the Tabu Search (TS) methodology that can be used in practice for actual carrier backbone networks. We validate our heuristic algorithm on a medium-sized network by comparing its results with the optimal solution (see Section VI-A.3).

TS is based on a partial exploration of the space of admissible solutions, starting from an initial solution usually obtained with a greedy algorithm, and ending when a stopping criterion is satisfied. The algorithm

returns the best solution it found during the entire search. For each admissible solution, the algorithm defines a class of neighboring solutions (the *neighborhood*) obtained from the current solution by applying an appropriate transformation, called a *move*. At each iteration of the TS algorithm, all solutions in the neighborhood of the current solution are evaluated, and the best one is selected as the current new solution.

In order to efficiently explore the solution space, the definition of neighborhood may change during the exploration of the solution space; this enables a *diversification* of the search in different solution regions. The TS algorithm can be seen as an evolution of the classical local optimum solution search algorithm called Steepest Descent ([27]). It can avoid getting trapped in local minima due to the TS mechanism that allows limited excursions toward solutions that appear worse than the current one.

The TS method introduces the use of a *Tabu list* to prevent the algorithm from cycling among already visited solutions. The Tabu list stores the latest accepted moves; as long as a move is stored in the Tabu list, it cannot be used to generate a new one. The choice of the Tabu list size is a key parameter of the optimization procedure: too small a size could cause the cyclic repetition of the same solutions, while too large a size can severely limit the number of applicable moves, thus preventing a good exploration of the solution space. The TS heuristic ends when a stopping criterion is reached. A common stopping criterion is simply to stop after some fixed number of iterations has been carried out.

A. Our Algorithm

We now state our algorithm by specifying how we implement each of the elements of a TS heuristic. We have added a preprocessing step that speeds up the rest of the search procedures.

1) *Preprocessing Step*. Generate the set of all admissible pairs of disjoint physical paths that could be used for each logical link. This determines the *admissible* solutions, each of which contains a particular mapping for each logical link. Admissibility here only refers to the fiber paths being disjoint.
2) *Initial Solution*. For each logical link, randomly select one pair of disjoint physical paths. Choose randomly within the pair which physical path is assigned as working path and which one is assigned as backup path. The aggregated BEP traffic flowing on each logical link can be sent either on the working path or on the back-up physical path. The path leading to the largest value of the objective function is chosen.
3) *Create Neighborhood*. Select a logical link at random. Keep the working path fixed and change the physical backup path. The set of all the admissible backup paths for the selected logical link defines the neighborhood of the current solution.

4) *Evaluation of Solutions in Neighborhood.* We need to evaluate each solution in the neighborhood and pick the best one. Only the solutions generated by selecting a *logical link* and *the pair of physical paths* not present in the Tabu List are analyzed during this step.
   a) Check the capacity of each solution to ensure that the protection requirements for the FP matrix are satisfied. If enough resources are not available on the two physical paths to protect the FP traffic, then the solution is discarded as infeasible.
   b) Determine an allocation of BEP traffic onto the spare bandwidth that maximizes our objective function. Consider putting BEP traffic on either the working or backup paths.
   c) Elect the best solution found in the neighborhood as new current solution.
5) *Update*. Update the Tabu list by adding the latest move used to generate the new current solution and removing the oldest. Update the best-solution-seen-so-far if the new current solution analyzed shows a larger value of the objective function F.
6) *Repeat.* If number of iterations is less than some predefined threshold, go to step 3, else stop.

We now comment on some of these steps in more detail. The move we apply to create the neighborhood has two nice properties. The first one is the guarantee that all solutions in this neighborhood are admissible [2]. The second property is that this kind of move makes it easy to implement a *diversification* step. For example, we can select a different number of logical links at each iteration, which will move up rapidly to another region of the solution space. We apply *diversification* only when a certain number of successive iterations fail to yield improvement. In our simulations this number is set to 50; when this number is reached we build a new solution by selecting a random number of logical links between 3 and 5. Note that after the diversification move has been done once, we return to the regular move based on perturbing a single logical link.

We check the feasibility of a solution (step 4a) by routing all the logical connections onto the logical topology using the standard OSPF IP routing protocol. Then each logical link (s, t) is routed over the physical topology using the physical paths selected by the TS metaheuristic. If sufficient resources are not available to protect the entire aggregated FP traffic on each logical link, then the solution is discarded. The next solution is then analyzed. Once we find a feasible solution, we move to step 4b.

After a solution is claimed *admissible* for the FP traffic, then the BEP traffic needs to be assigned to each logical connection. As we mentioned before, two fairness policies are implemented. The *MinG* policy requires that a minimum bandwidth $Z_{min} \geq 0$ is assigned to each logical connection for its BEP traffic. The

[2]Note that we distinguigh between *admissibility* that refers to two fiber paths being disjoint, and *feasibility* that refers to a set of paths having enough capacity to satisfy the protection needs

algorithm starts by routing all the logical connections into the logical topology using the OSPF IP routing algorithm, and by assigning Z_{min} BEP traffic to each connection. Then, the algorithm verifies if the available bandwidth for each logical link is larger than the aggregated FP and BEP traffic flowing on it. It this test is passed, all the single hop logical connections will get as much as they can, i.e. a further amount of BEP bandwidth equal to the remaining available capacity.

The second fairness policy, *MaxMin*, is implemented by a water-filling type algorithm as follows. The algorithm starts by routing all the logical connections into the logical topology using the OSPF IP routing algorithm, and by assigning zero BEP traffic to each connection. Then the amount of BEP traffic allocated to each connection is increased in equal increments until a logical link gets saturated. At this point, the BEP bandwidth allocated to all logical connections sharing this bottleneck is frozen (at an equal level for all of them). All the other connections, which do not share this bottleneck, can still receive additional BEP traffic, without impacting the bandwidth allocated to the frozen connections. We then proceed to increase in equal increments the bandwidth to all remaining unfrozen connections, until a new logical link becomes a bottleneck (i.e., saturated). The bandwidth assigned to connections traversing the new bottleneck are now frozen. The algorithm repeats until all the logical connections are frozen. At this point the bandwidth of each logical connection is determined by its own bottleneck.

We fix the size of the *Tabu list* to be 7. This number was chosen based upon our experience running simulations for different kinds of network topologies and FP traffic matrices. The searching procedure is stopped when a given number of iterations is reached. The number of iterations should be chosen relative to the size of the network and to achieve a good trade-off between computational time needed and the quality (distance from the optimal solution) of the solutions reached. We set this parameter to 1500 for the medium-sized network and 5000 for the large-sized network.

V. Class based scheduling at the IP layer

In this section we present a scheduler that is able to differentiate the two service classes in the event of a failure at the optical layer. The scheduler is depicted in Figure 2. Let C_l denote the capacity of logical link l during normal operation. A buffer of size B_l is available at the input of link l and is served at rate C_l. The space of this buffer can be managed by any policy (Drop-Tail, RED, etc.). By definition of our service classes, the simple best effort service is provided without any guarantees at this stage to any of the two classes.

When a fiber fails at the optical layer, all the logical links sharing this fiber will be switched from their primary paths to their backup paths. Each logical link l, affected by this failure, and whose backup path has

a smaller available capacity $C_l^* < C_l$, will experience a drop in bandwidth from C_l to C_l^*. Let CF_l and CB_l denote, respectively, the portion of C_l^* devoted to the aggregated FP and BEP traffic flowing on link l, and computed by the algorithms of Section IV.

After the drop in bandwidth from C_l to C_l*, packets of FP and BEP classes have to be served at rates CF_l and CB_l respectively. To maintain the same order for FP packets before and after the drop in bandwidth, we keep the buffer B_l (virtually) served at a rate C_l. We also place two parallel queues (one for each class) in between buffer B_l and the link l. After leaving the buffer B_l, a packet goes to its corresponding queue based on its class. The two queues are served in a weighted round-robin way with rates CF_l and CB_l (or with weights $WF_l = CF_l/C_l^*$ and $WB_l = CB_l/C_l^*$). The round-robin scheduler ensures a fine-granularity distribution of the bandwidth C_l^* between the two queues. The outputs of the two queues are connected to the link l whose bandwidth has dropped.

Our scheduler can be seen as the original buffer B_l extended with a Weighted Fair Queue buffer. The original buffer is always (virtually) served at the original rate C_l whereas the WFQ buffer is served at the real rate of the link. When the bandwidth of the link is equal to C_l, the WFQ buffer is transparent; packets of both classes are only queued in buffer B_l and they are served at a rate C_l[3]. This transparency is the result of the fact that the WFQ buffer is implemented in such a way as to be work conserving. When the bandwidth drops, the WFQ buffer automatically enters into action and starts to provide the differentiated service. If the peak rate of the FP traffic is less than CF_l, FP packets will only be queued in buffer B_l and get the same service as before the drop in bandwidth. BEP packets will be queued in both buffers B_l and WFQ, except if their peak rate is less than the available bandwidth.

Denote by BF_l and BB_l the two queues of the WFQ buffer for link l. We choose their sizes in a way that they absorb a full buffer B_l. That is,

$$BF_l = \frac{C_l - CF_l}{C_l} B_l, \qquad BB_l = \frac{C_l - CB_l}{C_l} B_l. \tag{2}$$

These two queues are managed according to the Drop-Tail policy. Other sizes and policies can also be used for these two buffers.

To illustrate the functioning of our scheduler, we simulate (using the *ns* simulator) a simple scenario where a link of 10 Mbps is crossed by an FP and a BEP traffic stream of 4 Mbps each. Both traffic flows are generated by UDP Poisson sources. The size of the buffer B_l is set to 50 packets and all packets are of 500 bytes. We start the simulation in the no-failure mode, then after 500 seconds, we emulate a failure that

[3]In order not to make a packet suffer two transmission times in B_l and on the link, we implement the buffer B_l in a way to deliver a packet at the beginning of its service time and not at its end as in classical queuing systems.

drops the bandwidth from 10 Mbps to 5 Mpbs. We stop the simulation after 1000 seconds. The weights of the scheduler are set as follows: $CF_l = 5Mbps$, $CB_l = 0$. We plot as a function of time the throughput of the FP and the BEP traffic averaged over 1 second intervals and we also plot the length of the queue in the three buffers of our scheduler. The plots are shown in Fig. 3 and 4. For the throughput, we see clearly that the FP traffic is not affected by the failure and how the BEP is penalized. For the queue length, the buffer at the first stage shows the same occupancy before and after the failure, whereas the buffers at the second stage are empty and transparent before the failure. After the failure, the FP buffer remains almost empty since the rate of the FP traffic is on average less than the available bandwidth 5 Mbps. The BEP buffer overflows after the failure since the BEP traffic is on average more than the bandwidth not used by FP. The FP traffic is then protected in terms of throughput and delay whereas the BEP traffic is penalized (less throughput, more delay and losses). This shows that our scheduler is achieving its goals.

VI. Numerical results

We now evaluate the performance of our two services proposal on a medium-sized network shown in Fig. 5, and on the large-sized Sprint backbone shown in Fig. 10 and 11. We first solve the mapping problem. Then, to study the performance degradation of both classes in case of physical link failures, we simulate each failure scenario in a network whose logical and physical topology are connected according to the output of our mapping solution. We use the *ns* simulator with our own implementation of our scheduler in each router. We remind to the reader that for large networks, such as Sprint backbone, we collapse all the intra-PoP routers in one single PoP-node and we consider the PoP as a large backbone router. For medium-size network we study the real router-to-router topology.

A. Mapping: Medium-Sized Heterogeneous Networks

We use the medium-size network shown in Fig. 5 whose WDM layer is quite heterogeneous. Three different WDM systems are implemented: some fibers are equipped with 16 channels at 200 Mbps, some with 16 channels at 120 Mbps and others with 16 channels at 50 Mbps. The line card speed limit for each logical link is set to 150 Mbps.

1) Topology Tradeoff Issue: We now quantify this tradeoff between optimizing for the no-failure-mode alone versus finding a good solution for single-failure-modes. We use an FP traffic matrix in which each element in the matrix (each logical connection) is assigned a random value uniformly between 0 and 100 Mbps. (We remind the reader that after we choose an initial matrix, we scale up the entire matrix, in

order to load the maximum amount of FP onto our network.) We look at three performance metrics: the amount of BEP traffic carried by the network in the no-failure mode S_0 (denoted $BEP(S_0)$), the minimum ($BEP(S_{mn})_{min}$) and the average BEP traffic ($BEP(S_{mn})_{av}$) carried by the network where the minimum and average are computed over all the single failure modes S_{mn}. These metrics are plotted in Fig. 6. This figure includes two graphs for two extreme values of the topology tradeoff parameter W, namely $W = 0$ (maximize the BEP traffic only for the no-failure mode) and $W = 1$ (maximize the average BEP traffic over all single failure scenarios without any consideration of the no failure mode). These graphs are plotted against the number of iterations executed by the TS heuristic. Before commenting on our performance metrics, we make an observation about the convergence of our heuristic algorithm. Although we limited the number of iterations of our algorithm to 1500 for the medium-sized network (Section IV), we see here that in all cases it typically takes no more than 30 to 40 iterations for our heuristic to converge.

In the case of $W = 0$, our algorithm would enable around 950 Mbps of BEP traffic to be carried in the network during no-failure-modes. The BEP traffic values in the figure are summed over all logical links and thus represents a network-wide BEP load. The load generated by FP traffic in this example was roughly 240 Mbps; hence our two-service class proposal combined with a good mapping solution, enables a network to increase its total carried load by a factor between 3 and 4. Since we optimized for the no-failure-mode only, when failures do happen, the average amount of BEP carried after a failure typically drops to around 250-300 Mbps. Some solutions lose 63% of the BEP traffic they enjoyed before the failure, while others can lose as much as 77%.

When we optimize for the failure modes ($W = 1$), we can see that during normal operation, the network carries roughly 650 Mbps of BEP traffic, and when a failure occurs this number typically drops to around 550 Mbps. Overall we carry approximately 21% less BEP traffic in normal operating conditions (S_0) when we optimize for failure modes instead of optimizing only for the no-failure mode. On the other hand, the BEP loss in the event of a failure is limited to around 23% when $W = 1$ as opposed to the 60-75% loss incurred when $W = 0$. This clearly indicates the tradeoff between optimizing for failure modes as opposed to non-failure modes.

2) Setting the value of the topology tradeoff parameter W: We now examine how the performance varies as a function of W as it ranges from 0 to 1. The metrics we examine here are the total network load carried including both FP and BEP traffic (shown in the left portion of Fig. 7), and the utilization of the links at the logical level (shown in the right portion of Fig. 7) where the utilization numbers again include both FP and BEP traffic.

We observe that by increasing W, the amount $BEP(S_0)$ of BEP traffic carried, under no-failure condi-

tions decreases, whereas the average amount $BEP(S_{mn})_{av}$ of BEP carried by the network in failure modes increases. This it what we would expect given our understanding of the topology tradeoff issue. The same behavior is true for the metric of logical link utilization - with the exception of the maximum utilization under the no-failure mode. This makes sense; the corresponding curve ($U(S_0)_{max}$) is always at 100% because there is always at least one link in the network at 100% utilization. We point out that without BEP traffic, the average logical link utilization would be around 18%. This is in the typical range at which carriers load their networks today. Carrier's do this as part of their overprovisioning approach which provides additional robustness to large failure events. Hence these results for our two-service proposal indicates that carriers could run their networks at much higher load levels (e.g., between 40-80% on average) *without* impacting today's clients who essentially use an FP service.

3) Validation of Heuristic: In this subsection we compare the performance of our heuristic algorithm to that of our optimal ILP solution (given in the Appendix). To do this over a multiplicity of cases, we first examined 50 different FP traffic matrices, each of which was generated using a uniform distribution. Then we generated another 50 traffic matrices whose entries where drawn from a negative exponential distribution with an average of 50 Mbps. Again each FP traffic matrix is scaled up as much as possible until some FP traffic connections reach their limit, and would no longer be protected on a 1:1 basis if we would continue to increase their allocated rate.

Results from this comparison are given in Fig. 8. The notation $MD - BEP(..)$ refers to the amount of BEP traffic carried in the solution found by our ILP model, while the notation $TS - BEP(..)$ refers to the amount of BEP carried in the solution found by our Tabu Search heuristic algorithm. In these figures we plot the FP and BEP loads separately. We can see for that all values of W and for both types of FP traffic matrices (uniform and negative exponential), the performance of the heuristic and the model are very close. For $W = 0$ the gap between the TS heuristic and the ILP model is less than 3%, while for $W = 1$ the gap is less than 5.8%, for both distributions.

B. Mapping: Large-Sized Heterogeneous Networks

We now examine how the previous results extend to a large-size network, such as Sprint backbone. Fig. 10 and 11 display the two simplified versions of the WDM and IP layers actually used in Sprint Backbone. The WDM layer consists of 36 OXC and 55 WDM fibers, while 18 PoPs and 36 logical links are present at the IP layer. Three different WDM systems are used, which we call W_a (40 channels at 10 Gbps), W_b (40 channels at 2.44 Gbps) and W_c (40 channels at 622 Mbps). Each IP PoP has an electronic speed equal to 2.4 Gbps.

1) Basic Results: We ran our Tabu Search heuristic for the Sprint backbone using 15 traffic matrices randomly generated from a uniform distribution between 0 and 100 Mbps as described previously. Our two metrics of load levels carried and logical link utilization are shown in Fig. 12. The general results are similar to those obtained for the medium-sized network.

For all values of W, the amount of BEP traffic carried during no failure scenarios ranges from 55 to 60 Gbps. This corresponds to an increase in the carried load of a factor of 9 to 10, as compared to a network carrying FP alone. In the event of a failure, the average amount of BEP lost ranges from 30 to 50%. Even in the most conservative case ($W = 1$), we can support a BEP service carrying approximately 55 Gbps of traffic, and the performance degradation suffered by BEP during failure events is approximately the loss of 1/3 of its traffic. In this case, the average logical link utilization is around 70% during normal operation and drops to roughly 40% during failure modes.

2) Impact of the Fairness Policies: We now examine the difference in terms of BEP network load carried by each logical connection when the two fairness policies are implemented. On the top and middle of Fig. 9 we show the BEP bandwidth in Mbps (y-axis) assigned to each logical connection (x-axis) by using respectively the *MinG* policy and the *MaxMin* policy. The bottom of Fig. 9 shows the cumulative distribution of the two fairness policies, i.e. the fraction of logical connections (y-axis) with an assigned bandwidth less than or equal to a specific value (x-axis). The case shown is for $W = 0.7$ and $Z_{min} = 25$ Mbps.

First, note that the minimum BEP bandwidth assigned to each connection is greater than or equal to $Z_{min} = 25$ Mbps[4]. By looking at the number of OD (Origin-Destination) pairs with a BEP load larger than 25 Mbps, we can see from these figures that the *MinG* policy assigns almost 80% of the logical connections to the minimum value, while the *MaxMin* policy assigned only 60% of its logical connections to 25 Mbps. This can also be seen by looking at the bottom plot for the case when the x-axis value is at 25 Mbps. This is the first indication that the *MaxMin* policy provides better fairness (as it is supposed to do). By looking at the bottom plot, we can also observe that the *MinG* policy is nearly flat in the range of 25 to 1600 Mbps, indicating that very few OD pairs have values in that range, while the *MaxMin* curve does have gradual change and growth in that bandwidth range. It is also clear from the top two plots that the *MaxMin* policy has more OD pairs with values in the 100-1000 Mbps range. This is the second indication that the *MaxMin* policy yields better fairness than a *MinG* policy. We computed the total load carried in the two fairness policies, and the *MaxMin* policy carries 14% less load than the *MinG* policy. Hence the tradeoff between these two policies is that increasing fairness leads to a reduction in overall total load carried.

[4]This characteristic is not visible from the top and the middle of Fig. 9 because of the large y-axis range, but is clear by looking at the bottom of Fig. 9

C. IP scheduler: simulation results

We now examine the on-line performance of our proposed schemes. We study the medium-sized network shown in Fig. 5 and implement our scheduler in each of the routers. The performance of both classes of service was evaluated using the *ns simulator.* We remind the reader that to assess the performance of the two classes of service in case of a physical link failure, we need to know exactly which sequence of physical links are used by each logical link. For this purpose, we implement the solution obtained by solving the mapping problem for this topology, using the heuristic proposed in Section IV. Between each pair of routers, we set the two *average* traffic flow rates (for FP and BEP traffic) according to the values used in the previous uniform traffic matrix. We use this average rate for each logical connection as the mean of a Poisson distribution so that packets arrivals are generated according to a Poisson process. We take Poisson traffic for its simplicity and for its good approximation of Internet traffic in IP backbone networks [28]. The traffic is symmetric in that two routers exchange the same amount of traffic in both directions. We assume each logical link to have 150 Mbps card speed. We take all logical link delays equal to 10 ms, and we set the packet size of FP and BEP packets to 1500 bytes. All simulations are run for a long duration of 1000 seconds.

First we run a simulation for the no failure case. Between each pair of routers, we measure the throughput, loss and delay of FP and BEP traffic. With 8 IP layer routers, we have 8*7=56 router pairs. Since the logical connections are symmetric, we group bidirectional traffic into a single router pair. We have thus 28 such pairs. We also measure the aggregate throughput on each logical link. Next, we run a simulation for each failure scenario. Seventeen failure scenarios are considered in total, numbered from 1 to 17, with the no failure scenario numbered 0. Every failure causes a drop of the total bandwidth available for logical links. Logical links are symmetric in all failure scenarios. Fig. 13 summarizes these drops in bandwidth. The lines in this figure correspond to logical links (13 in total). The x-axis represents the index of the failure scenario considered. The y-axis represents the total bandwidth available on a logical link in a failure scenario. For all failure scenarios we redo the same measurements as in the first simulation, run for the no failure case, namely: (i) throughput, delay and losses between router pairs, and (ii) aggregate throughput on every logical link. Using these measurements we can study the impact of a fiber failure on each class of service at the IP layer in terms of throughput (Fig. 14 and 15), delay (Fig. 16 and 17) and loss (Fig. 18 and 19). For all these figures, the x-axis shows the performance of the traffic in the no failure mode and the y-axis shows the performance of the traffic in the failure mode. The number of points in each figure is equal to the number of failure scenarios (17) times the number of router pairs (28).

In the throughput plot for the FP traffic (Fig. 14), all the points lie around the diagonal. This indicates that the throughput for FP traffic is not impacted by single link failures. In the case of delay and loss (Fig.16 and 18) there are just a few points that are a bit above the diagonal. Note that this would happen even without the addition of BEP traffic. When the bandwidth drops during a failure, the transmission time of FP packets increases so we cannot avoid an increase in the packet delay even if the average FP traffic is less than the available bandwidth in the failure mode. For the loss, it is the same thing since buffers are finite and the traffic at the packet level is Poisson (more bursty than constant bit rate). These figures show that our mapping solution and scheduler are working properly in that they achieve their goal of adding BEP traffic into the network without impacting the SLA of the FP traffic.

For the BEP traffic there is clearly a degradation of service in the failure modes. This is evidenced by the points below the diagonal in the throughput plot[5] and by the points above the diagonal in the delay and loss plots. When throughput drops occur during failure periods, the overall throughput of BEP load is reduced between 30%-60% depending upon the particular failure scenario. Many points in the BEP figures continue to lie around the diagonal which means that some BEP flows are not affected by the corresponding failure and they continue to receive the same service as in the no failure mode.

We also show the aggregate throughput of FP and BEP traffic on logical links and compare it between the failure mode and the no failure mode. For each logical link between two neighboring routers and for each failure scenario, we measure the aggregate throughput for both FP and BEP. We plot the results in Figure 20 for FP traffic and in Figure 21 for BEP traffic. The x-axis in the figures show the failure scenario number and the y-axis the aggregate throughput in Mbps. The lines in the figures correspond to logical links of the network topology in Figure 5. It is clear from the figures that the aggregate FP throughput remains constant on all logical links for all failure scenarios, and equal to its value in the no failure mode (obtained by looking at the y-axis for the scenario numbered). This is another metric indicating the success of our mapping and scheduler solutions. The aggregate BEP throughput degrades only on some logical links in some failure scenarios, and the amount of BEP degradation is dictated by how much bandwidth is available on a logical link after failure.

VII. Concusions

In this paper we have solved both a mapping problem and a scheduling problem that carriers would need to resolve in order to support two classes of service differentiated by their level of protection. We

[5]The throughput values in this plot range from 0 to 10 Mbps while those in Fig. 7 and 8 range up to 1000 Mbps because in Fig. 15 we plot throughputs per router pair while in Fig. 7 and 8, BEP traffic is given network-wide (the sum of all router pairs).

illustrated that our heuristic solution, that scales to large networks, performs within 3-5% of an optimal solution. The multifaceted version of the problem we considered engenders a variety of important tradeoffs that we illustrated and quantified. For example, we showed that in order to provide service degradation rather than total service disruption one needs to incorporate failure scenarios inside the optimization steps. However ensuring that the throughput drops for BEP traffic during failure are limited, also implies that during normal operation the total BEP throughput carried is less than would be if we did not consider failures inside the optimization solution. In the large network scenario we examined, when we include failures in the optimization we carry roughly 8% less BEP traffic than if we don't. However, the gain is that we also drop 22% less BEP during failure episodes than if we didn't consider failures. This is clearly worth the tradeoff because even when including failure events, the total load carried by a network (with both FP and BEP services) is roughy a factor of ten more than the load carried by a network supporting FP alone.

Because the pockets of additional bandwidth in carrier networks are usually unevenly distributed, straightforward solutions for offering BEP bandwidth to logical connections would lead to unfair partitions of bandwidth. To compensate we enforced a max-min fairness policy and showed that this does improve the fairness of the BEP bandwidth partition over simple fairness policies such as a minimum bandwidth allocation. More importantly, we illustrated that this carrier requirement also induces an important tradeoff on the amount of BEP a network can carry. The more fairness that is required, the less total BEP traffic can be carried. For the two fairness policies we examined, providing max-min fairness instead of a minimum guarantee, means that the BEP traffic load carriable drops by 14%.

Our approach is both practical and complete because we provide a scalable heuristic that converges quickly and because we provide a scheduling solution for on-line usage. Our combined solutions to the mapping and scheduling problems yields a system in which the SLAs of the FP traffic are not affected by the addition of BEP, the total load carried on backbone networks is increased by a factor from 3 to 10 (depending upon the network scenario considered). We avoided a total disruption in the BEP traffic and limited the degradation to be in the range of a 30-60% drop in throughput. Thus BEP users will experience slower connections but not a complete disruption.

In summary, we have illustrated that carrier requirements often lead to restrictions in the total amount of BEP traffic than can be carried. The good news is that even when one meets these load limiting policies, there is still a great deal of BEP traffic than can be carried and hence carrier networks contain a large potential to increase their current carried load.

REFERENCES

[1] S. Casner, A. Alaettinoglou, "Detailed Analysis of ISIS Routing Protocol in the QWEST Backbone", *NANOG Presentation*, February, 2002.

[2] G. Iannaccone, C. Chuah, S. Bhattacharyya and C. Diot, "Analysis of Link Failures in an IP Backbone", Proc. of ACM Sigcomm Internet Measurement Workshop, November, 2002.

[3] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C. Chuah and C. Diot, "Characterization of Failures in an IP Backbone", *Proc. of IEEE Infocom*, Hong Kong, March, 2004.

[4] A. Autenrieth and A. Kirstdter, "Fault-Tolerance and Resilience Issues in IP-Based Networks", *Second International Workshop on the Design of Reliable Communication Networks (DRCN)*, April 2000.

[5] P. Bonenfant, "Optical layer survivability: a comprehensive approach," *Proc. OFC '98*, San Jose, CA, vol. 2, pp. 270-271, February 1998.

[6] B. Van Caenegem, W. Van Parys, F. De Turck and P. Demeester, "Dimensioning of survivable WDM networks", *IEEE Journal on Selected Areas in Communications*, Vol. JSAC-16(7), pp. 1146-1157, September 1998.

[7] D. Colle et al, "Data-centric Optical networks and their survivability", *IEEE Journal on Selected Areas in Communications*, Vol. JSAC-20(1), pp. 6–20, January 2002.

[8] P. Demeester et al, "Resilience in a multi-layer network", *IEEE Communications Magazine*, vol. 37(8), pp. 70–76, August 1999.

[9] H. Zhang and A. Durresi, "Differentiated Multi-Layer Survivability in IP/WDM Networks", *Proc. NOMS'02*", pp. 681–694, April 2002.

[10] K. Papagiannaki, S. Moon, C. Fraleigh, P. Thiran, F. Tobagi and C. Diot, "Analysis of Measured Single-Hop Delay from an Operational Backbone Network", *Proc. of IEEE Infocom*, New York, June, 2002.

[11] J. Moy, "Open Shortest Path First Version 2", *RFC 2178*, July 1997.

[12] ISO, "Intermediate System to Intermediate System (IS-IS) Intra-Domain Routing Exchange Protocol", International Standard 10589:2002, Second Edition, 2002.

[13] A. Fumagalli, L. Valcarenghi, "IP Restoration vs. WDM Protection: Is there an Optimal Choice?", *IEEE Network*, pp.34-41, November/December 2000.

[14] O. Gerstel, R. Ramaswami, "Optical Layer Survivability: A Services Perspective", *IEEE Communication Magazine*, 38(3) pp.104-113, 2000.

[15] R. Ramamurthy, B. Mukherjee, "Survivable WDM Mesh Networks", *Proc. Infocom 1999*, New York, March 1999.

[16] G. Mohan, A.K. Somani,. "Routing Dependable Connections with Specified Failure Restoration Guarantees in WDM Networks", *Proc. Infocom 2000*, Jerusalem, April 2000.

[17] M. Sridharan, A.K. Somani, "Revenue Maximization in Survivable WDM Networks", *Opticomm 2000*, Dallas, October 2000.

[18] A. Nucci, N. Taft, P. Thiran, H. Zhang and C. Diot, "Increasing Link Utilization in IP over WDM Networks", *Opticomm 2002*, Boston, Massachussets (USA), July 2002.

[19] J. Armitage, O. Crochat, J.Y.Le Boudec, "Design of a Survivable WDM Photonic Network", *in Proc. INFOCOM 1997*, pp. 244-252, April 1997. Boston, Massachussets (USA), July 2002.

[20] O. Crochat, J.Y.Le Boudec, "Design Protection for WDM Optical Networks", *IEEE Journal on Selected Areas in Communication*, Vol. 16, N. 7, pp. 1158-1165, September 1998.

[21] O. Crochat, J.Y.Le Boudec, O. Gerstel, "Protection Interoperability for WDM Optical Networks", *IEEE Transaction on Networking*, Vol. 8, N. 3, pp. 384-395, June 2000.

[22] E. Modiano, A. Narula-Tam "Survivable routing of logical topologies in WDM networks", *Infocom 2001*, Vol. 1, pp. 348-357, Anchorage, April 2001.

[23] F. Giroire, A. Nucci, N. Taft, C. Diot, "Increasing the Robustness of IP Backbones in the Absence of Optical Level Protection", *Infocom 2003*, San Francisco, California (USA), March 2003.

[24] A. Nucci, B. Sanso, T.G. Crainic, E. Leonardi, M.A. Marsan, "Design of Fault-Tolerant Logical Topologies in Wavelength-Routed Optical IP Networks", *Globecom 2001*, San Antonio, Texas (USA), November 2001.

[25] CPLEX, “ILOG CPLEX Software Optimization Suite”, *http://www.ilog.com/products/cplex/*.

[26] F. Glover, M. Laguna, “Tabu Search”, *Kluwer Academic Publishers 1997*.

[27] G.L. Nemhauser, A.H.G. Rinnoy Kan, M.J. Todd, “Optimization - Handbooks in Operations Research and Management Science”, *North-Holland*, Vol.1, 1989.

[28] Jin Cao, William S. Cleveland, Dong Lin, and Don X. Sun. On the nonstationarity of internet traffic. In Proceedings of ACM SIGMETRICS, pages 102–112, 2001.

APPENDIX (Included only for review purposes)

We formulate the mapping problem as an Integer Linear Program (ILP) whose objective is to maximize the objective function F. We focus on the 1:1 protection strategy, however a model for the 1+1 scheme can be easily derived from our 1:1 model. In the following we refer to *network state* as the condition in which the network can be at any time. We denote by S_{mn} the state of the network after the failure of the physical link (m, n) connecting nodes m and n in the physical topology. We denote by S_0 the state of the network when there is no failure at all in the network. If the number of physical links is M, there are thus $(M + 1)$ different states. In the following we use the *Minimum Fairness Guaranteed* policy (MinG).

A. Notation for the given input data

The super-index indicates the layer, starting by the lowest layer, zero, that represents the physical network. Let $G^0 = (V, E^0)$ be the unidirectional graph representing the physical topology. It is composed of OXC nodes V interconnected by optical fibers (i, j), whose set is denoted by E^0. Let $|V| = N$ be the cardinality of set V and $|E^0| = M$ be that of set E^0. We assume that each fiber $(i, j) \in E^0$ is described by the pair of parameters $\{n_{ij}$,$c^f_{ij}\}$, where n_{ij} represents the number of parallel WDM channels, having all the same bandwidth equal to c^f_{ij}. Let $G^1 = (U, E^1)$ be the unidirectional graph representing the logical topology. It is composed of IP routers U interconnected by lightpaths (s, t), whose set is denoted by E^1. Let $|U| = K$ be the cardinality of set U and $|E^1| = H$ be that of set E^1. Let c^l_{st} be the capacity associated with the logical link $(s, t) \in E^1$. Let $\mathcal{S}$ be the set of all the possible network states whose cardinality is $|\mathcal{S}| = M+1$, in which the no failure state is indicated by S_0 and the failure states by S_{mn} (where $(m, n) \in E^0$ indicates which fiber is broken). Let $\mathcal{C} = \{(k, h)\}$ be the set of all the logical connections (k, h). Let $D_{FP} = [d^{kh}(FP)] \geq 0$ be the FP traffic matrix, where each entry $d^{kh}(FP)$ describes the FP traffic associated with each logical connection $(k, h) \in \mathcal{C}$. Let $\mathcal{R} = [r^{kh}_{st}]$ be the set of routes for each logical connection $(k, h) \in \mathcal{C}$ at the IP layer; $r^{kh}_{st} = 1$ if the logical connection (k, h) uses the logical link $(s, t) \in E^1$ in its own path, and 0 otherwise. For clarity of notation, in the following ILP formulation, the aggregated FP traffic on each logical link $(s, t) \in E^1$ will be described by $f^{st}(FP) = \sum_{(k,h)\in\mathcal{C}} r^{kh}_{st} d^{kh}(FP)$. Let Z_{min} represent the minimum amount of bandwidth assigned to each logical connection for its BEP traffic.

B. Notation for the decision variables

For uniformity of notation, let $D_{BEP}(S) = [d^{kh}_S(BEP)] \geq 0$ be the BEP traffic matrix associated with the network state $S \in \mathcal{S}$ where each entry $d^{kh}_S(BEP)$ represents the BEP traffic exchanged between the IP OD pair (k, h) in the network state S. Then the aggregated BEP traffic on each logical link (s, t) for each

network state $S \in \mathcal{S}$ will be described by the variables $f_S^{st}(BEP) = \sum_{(k,h)\in\mathcal{C}} r_{st}^{kh} d_S^{kh}(BEP)$. For each logical link (s,t) two disjoint physical paths are required. Let w_{ij}^{st} and b_{ij}^{st} be two binary variables used to describe the routing for the logical link (s,t) over the physical topology G^0, respectively for the working and the backup physical paths. The variables w_{ij}^{st} (b_{ij}^{st}) are equal to 1 if the physical link $(i,j) \in E^0$ is crossed by the working (backup) physical path associated with the logical link $(s,t) \in E^1$ and 0 otherwise. Let $\alpha_{ij}^{st}(BEP) \geq 0$ and $\beta_{ij}^{st}(BEP) \geq 0$ be the BEP traffic flow variables associated respectively with the working and backup physical paths for the logical link $(s,t) \in E^1$. They describe respectively the amount of aggregated BEP traffic flowing on the working and backup path in the no failure state S_0. Let ϵ^{st} be the binary variables used to choose the routing of BEP traffic. The model described here considers the most general case where the BEP traffic could flow either on the working path or on the backup path but cannot be split between them. This is the reason why we have to introduce the ϵ^{st} variables that are equal to 1 if the BEP traffic associated with the logical link $(s,t) \in E^1$ is routed on the working path and equal to 0 if it is routed on the backup path.

Since we consider all the network states, it is necessary to introduce variables that describe exactly the network behaviour in each failure state S_{mn}. We define first the variables $\nu_{ij}^{st}(m,n) \geq 0$ and $\mu_{ij}^{st}(m,n) \geq 0$ to describe the FP traffic redirection and the variables $\sigma_{ij}^{st}(m,n) \in \{0,1\}$, $\delta_{ij}^{st}(m,n) \in \{0,1\}$ and $\tau_{ij}^{st}(m,n) \geq 0$ to describe the paths on which the BEP traffic is sent to and its amount. When a fault occurs in the network, the primary paths carring the FP traffic in the no failure state may or may not be involved. When a primary path fails, it is necessary to switch the FP traffic to its backup path. The variables $\nu_{ij}^{st}(m,n)$ indicate the amount of FP traffic flowing on the logical link (s,t), and switched to the backup path (i,j) since the fault of the physical link (m,n) involved its primary path. Instead when the primary path does not pass through the fiber fault, it is still able to carry the FP traffic. In that case, the amount of FP traffic flowing on the primary path (i,j) is equal to that carried in the no failure state ($f^{st}(FP)$) and it is represented by the variables $\mu_{ij}^{st}(m,n)$. With regard to BEP traffic, the binary variables $\sigma_{ij}^{st}(m,n)$, are used to evaluate if the backup physical path used by the logical link (s,t) passes through the broken fiber (m,n) and its primary path uses the physical link (i,j). The binary variables $\delta_{ij}^{st}(m,n)$ indicate the available links that can be used to carry the BEP traffic when both of the primary and backup paths are not involved in the failure (m,n). Note that, for each failure state, it is necessary to solve the routing problem for the BEP traffic to evaluate the new BEP load carried by each logical. Finally the variables $\tau_{ij}^{st}(m,n) \geq 0$ describe the new amount of aggregated BEP traffic flowing on each fiber $(i,j) \in E^0$ for each logical link $(s,t) \in E^1$ in each failure state S_{mn}.

C. Objective function

We can now formally define the objective function $\mathcal{F}$ that we want to maximize. Remember that $W \in [0,1]$ is a parameter weighting the importance of the BEP traffic load that can be routed in the network in the absence of failure, versus the average amount of BEP traffic that can be restored in the network after the occurrence of a single link failure. This functional reads

$$\mathcal{F} = (1-W) \sum_{(k,h)\in\mathcal{C}} d_{S_0}^{kh}(BEP) + \frac{W}{|S_{mn}|} \sum_{(k,h)\in\mathcal{C},(m,n)\in E^0:m<n} d_{S_{mn}}^{kh}(BEP) \tag{3}$$

This maximization needs of course to be done under the appropriate set of constraints. We can divide them in two sets. The first one gathers all the constraints applicable in the non failure state S_0. They were originally derived in [18], we restate them in the next subsection to keep the paper self-contained. The second set groups all the new additional constraints that apply to the various single failure states S_{mn}.

D. Constraints in the no failure state

Having defined the variables above, we can now state all the constraints linking them in the no failure state S_0.

• The minimum amount of BEP traffic assigned to each logical connection:

$$d^{kh}(BEP) \geq Z_{min} \quad \forall (k,h) \in \mathcal{C} \tag{4}$$

Relation (4) ensures that the guaranteed minimum fairness requirement in satisfied because these constraints force each logical connection to get at least an amount Z_{min} of bandwidth for its BEP traffic.

• The aggregated BEP traffic on each logical link (s,t) is:

$$f_{S_0}^{st}(BEP) = \sum_{j\in V:(s,j)\in E^0} (\alpha_{sj}^{st}(BEP) + \beta_{sj}^{st}(BEP)) \quad \forall (s,t) \in E^1 \tag{5}$$

Relation (5) ensures that the aggregated BEP traffic associated with each logical link (s,t) leaving node s can only traverse either the backup or working path at the WDM layer for each logical link. This general equation allows the traffic to be sent on either the working ($\alpha_{sj}^{st}(BEP)$) or the backup ($\beta_{sj}^{st}(BEP)$) path. Later we add a constraint that enables one of the two be selected, but not both (because we do not support traffic splitting).

• The flow continuity constraint for the physical working path associated with logical link (s,t) is:

$$\sum_{j\in V:(i,j)\in E^0} w_{ij}^{st} - \sum_{j\in V:(j,i)\in E^0} w_{ji}^{st} = \begin{cases} 1 & \text{if} \quad i=s \\ -1 & \text{if} \quad i=t \\ 0 & \text{otherwise} \end{cases} \qquad (6)$$
$$\forall i \in V, \forall (s,t) \in E^1$$

• The flow continuity constraint for the physical backup path associated with logical link (s,t) is:

$$\sum_{j\in V:(i,j)\in E^0} b_{ij}^{st} - \sum_{j\in V:(j,i)\in E^0} b_{ji}^{st} = \begin{cases} 1 & \text{if} \quad i=s \\ -1 & \text{if} \quad i=t \\ 0 & \text{otherwise} \end{cases} \qquad (7)$$
$$\forall i \in V, \forall (s,t) \in E^1$$

Equations (6) and (7) define the two physical paths associated with each logical link.

• We force the working and backup paths to be disjoint by the following constraint:

$$w_{ij}^{st} + w_{ji}^{st} + b_{ij}^{st} + b_{ji}^{st} \leq 1 \quad \forall (i,j) \in E^0, \quad \forall (s,t) \in E^1, \qquad (8)$$

• The BEP traffic flowing on the working and backup paths of logical link (s,t) is constrained by:

$$\alpha_{ij}^{st}(BEP) \leq B w_{ij}^{st} \quad \forall (i,j) \in E^0, \forall (s,t) \in E^1 \qquad (9)$$

$$\beta_{ij}^{st}(BEP) \leq B b_{ij}^{st} \quad \forall (i,j) \in E^0, \forall (s,t) \in E^1 \qquad (10)$$

where B is a large number chosen so that it is larger than $\alpha_{ij}^{st}(BEP)$ for any $(i,j) \in E^0$ and any $(s,t) \in E^1$. For example, we can take

$$B = \max_{(i,j)\in E^0, i<j} \left\{ c_{ij}^f \right\}. \qquad (11)$$

Relation (9) forces $\alpha_{ij}^{st}(BEP)$ to be equal to 0 if $w_{ij}^{st} = 0$, that is, if the working path selected for the logical link (s,t) does not cross over fiber (i,j). On the other hand, if $w_{ij}^{st} = 1$, then relations (9) do not impose any restriction on $\alpha_{ij}^{st}(BEP)$. The same holds for Relation (10). The same number B will be used later on for several relations.

• The following two equations determine which of the two physical paths will carry the BEP traffic.

$$\alpha_{ij}^{st}(BEP) \leq \epsilon^{st} c_{ij}^f \qquad \forall (s,t) \in E^1 \qquad (12)$$
$$\beta_{ij}^{st}(BEP) \leq (1-\epsilon^{st}) c_{ij}^f \qquad \forall (s,t) \in E^1 \qquad (13)$$

The above equations (12) and (13) determine which of the two physical paths will carry the BEP traffic. Recall that only one path at a time is allowed to carry BEP. If $\epsilon^{st} = 0$ the BEP trafic will be sent to the backup path otherwise it will be sent to the working path.

• Flow continuity constraints for the BEP class of service carried by logical link (s,t) on the selected physical path (working or backup) are:

$$\begin{aligned}
&\sum_{j\in V:(i,j)\in E^0} (\alpha_{ij}^{st}(BEP) + \beta_{ij}^{st}(BEP)) - \\
&\sum_{j\in V:(j,i)\in E^0} (\alpha_{ji}^{st}(BEP) + \beta_{ji}^{st}(BEP)) \\
&= \begin{cases} f_{S_0}^{st}(BEP) & \text{if} \quad i = s \\ -f_{S_0}^{st}(BEP) & \text{if} \quad i = t \\ 0 & \text{otherwise} \end{cases} \\
&\forall i \in V, \forall (s,t) \in E^1
\end{aligned} \tag{14}$$

• The maximum number of wavelengths on each physical fiber is constrained by:

$$\sum_{(s,t)\in E^1} (w_{ij}^{st} + w_{ji}^{st} + b_{ij}^{st} + b_{ji}^{st}) \leq n_{ij} \quad \forall (i,j) \in E^0 : i < j \tag{15}$$

Equation (15) ensures that the number of logical channels traversing each fiber cannot be larger than the number of available wavelengths.

• We have the following capacity constraints from the physical layer:

$$\begin{aligned}
&f^{st}(FP)(w_{ij}^{st} + w_{ji}^{st}) + \alpha_{ij}^{st}(BEP) + \alpha_{ji}^{st}(BEP) \leq c_{ij}^{f} \\
&\forall (i,j) \in E^0 : i < j, \forall (s,t) \in E^1
\end{aligned} \tag{16}$$

$$\begin{aligned}
&f^{st}(FP)(b_{ij}^{st} + b_{ji}^{st}) \leq c_{ij}^{f} \\
&\forall (i,j) \in E^0 : i < j, \forall (s,t) \in E^1
\end{aligned} \tag{17}$$

$$\begin{aligned}
&\beta_{ij}^{st}(BEP) + \beta_{ji}^{st}(BEP) \leq c_{ij}^{f} \\
&\forall (i,j) \in E^0 : i < j, \forall (s,t) \in E^1
\end{aligned} \tag{18}$$

Relation (16) ensures that there is enough capacity on the working path to carry the FP traffic and eventually BEP. Relation (17) ensures that there is enough capacity on the backup path to protect the FP traffic flowing on the working path, and relation (18) ensures that the maximum amount of BEP traffic sent on the backup path cannot exceed the capacity of the WDM channel used in the corresponding fiber.

• Capacity constraints from the logical layer:

$$f^{st}(FP) + f_{S_0}^{st}(BEP) \leq c_{st}^{l} \quad \forall (i,j) \in E^0 : i < j \tag{19}$$

Relation (19) ensures that the total amount of traffic carried by each logical channel is not larger than its own capacity dictated by its electronic speed of its interface.

E. Constraints in the single failure states

Let us now add the constraints for the variables related to the failure states S_{mn}, which correspond the state of the network after the failure of the physical link (m,n).

• We capture the switching of FP traffic from working to backup paths as follows:

$$\begin{gathered}\nu_{ij}^{st}(m,n) \leq B(w_{mn}^{st} + w_{nm}^{st}) \\ \forall (i,j),(m,n) \in E^0 : m < n, \forall (s,t) \in E^1\end{gathered} \tag{20}$$

$$\begin{gathered}\nu_{ij}^{st}(m,n) \leq B b_{ij}^{st} \\ \forall (i,j),(m,n) \in E^0 : m < n, \forall (s,t) \in E^1\end{gathered} \tag{21}$$

$$\begin{gathered}\nu_{ij}^{st}(m,n) \geq f^{st}(FP) - (2 - (w_{mn}^{st} + w_{nm}^{st} + b_{ij}^{st}))B \\ \forall (i,j) \in E^0, \forall (m,n) \in E^0 : m < n, \forall (s,t) \in E^1\end{gathered} \tag{22}$$

$$\begin{gathered}\nu_{ij}^{st}(m,n) \leq f^{st}(FP) \\ \forall (i,j),(m,n) \in E^0 : m < n, \forall (s,t) \in E^1\end{gathered} \tag{23}$$

$$\sum_{(s,t)\in E^1,(m,n)\in E^0 : m<n} (\nu_{mn}^{st}(m,n) + \nu_{nm}^{st}(m,n)) = 0 \tag{24}$$

Relations (20) to (24) redirect the FP traffic from the working path to the backup path if the working path is involved in the failure of the fiber (m,n). The variable $\nu_{ij}^{st}(m,n)$ represents the new amount of FP traffic flowing on the backup path; it is therefore equal to the total amount of FP traffic on logical link (s,t), $f^{st}(FP)$, if both $(w_{mn}^{st} + w_{nm}^{st}) = 1$ and $b_{ij}^{st} = 1$, and it is 0 otherwise.

• If the working path is not involved in the failure, then no switching of FP traffic from working to backup paths is needed.

$$\begin{gathered}\mu_{ij}^{st}(m,n) \geq f^{st}(FP) w_{ij}^{st} - B(w_{mn}^{st} + w_{nm}^{st}) \\ \forall (i,j) \in E^0, \forall (m,n) \in E^0 : m < n, \forall (s,t) \in E^1\end{gathered} \tag{25}$$

$$\begin{gathered}\mu_{ij}^{st}(m,n) \leq f^{st}(FP) w_{ij}^{st} \\ \forall (i,j),(m,n) \in E^0 : m < n, \forall (s,t) \in E^1\end{gathered} \tag{26}$$

$$\begin{gathered}\mu_{ij}^{st}(m,n) \leq (1 - (w_{mn}^{st} + w_{nm}^{st}))B \\ \forall (i,j) \in E^0, \forall (m,n) \in E^0 : m < n, \forall (s,t) \in E^1\end{gathered} \tag{27}$$

$$\sum_{(s,t)\in E^1,(m,n)\in E^0 : m<n} (\mu_{mn}^{st}(m,n) + \mu_{nm}^{st}(m,n)) = 0 \tag{28}$$

Relations (25) to (28) constrain the FP traffic to follow the working path when it is not involved in the failure of fiber (m,n). The variables $\mu_{ij}^{st}(m,n)$ are forced to be equal to $f^{st}(FP)$ for the same fibers (i,j) used by the working path ($w_{ij}^{st}=1$) when the working path is not involved into the failure S_{mn} (($w_{mn}^{st}+w_{nm}^{st})=0$).

• Definition of new physical paths allowed to send BEP traffic in case of failure, when *only* the backup path of the logical link is involved in the failure:

$$\begin{gathered}\sigma_{ij}^{st}(m,n)\leq b_{mn}^{st}+b_{nm}^{st}\\ \forall(i,j),(m,n)\in E^0:m<n,\forall(s,t)\in E^1\end{gathered}\tag{29}$$

$$\begin{gathered}\sigma_{ij}^{st}(m,n)\leq w_{ij}^{st}\\ \forall(i,j),(m,n)\in E^0:m<n,\forall(s,t)\in E^1\end{gathered}\tag{30}$$

$$\begin{gathered}\sigma_{ij}^{st}(m,n)\geq(b_{mn}^{st}+b_{nm}^{st}+w_{ij}^{st}-1)\\ \forall(i,j)\in E^0,\forall(m,n)\in E^0:m<n,\forall(s,t)\in E^1\end{gathered}\tag{31}$$

$$\sum_{(s,t)\in E^1,(m,n)\in E^0:m<n}(\sigma_{mn}^{st}(m,n)+\sigma_{nm}^{st}(m,n))=0\tag{32}$$

Relations (29) to (32) define the new physical paths for each logical link (s,t) allowed to carry BEP traffic when only its backup path associated with (s,t) is involved into the failure S_{mn}. Then the BEP traffic has to be sent on the working path associated with (s,t). All this information is kept in the variables $\sigma_{ij}^{st}(m,n)$, which are equal to 1 if the backup path of the logical link (s,t) is involved in the failure of fiber (m,n) ($b_{mn}^{st}+b_{nm}^{st}=1$) and if its working path uses fiber (i,j) ($b_{ij}^{st}=1$), and to 0 otherwise.

• Definition of new physical paths allowed to send BEP traffic in case of failure, when *both* the working and backup paths of the logical link are involved in the failure:

$$\begin{gathered}\delta_{ij}^{st}(m,n)\leq 1-(w_{mn}^{st}+b_{mn}^{st}+w_{nm}^{st}+b_{nm}^{st})\\ \forall(i,j)\in E^0,\forall(m,n)\in E^0:m<n,\forall(s,t)\in E^1\end{gathered}\tag{33}$$

$$\begin{gathered}\delta_{ij}^{st}(m,n)\leq(w_{ij}^{st}+b_{ij}^{st})\\ \forall(i,j)\in E^0,\forall(m,n)\in E^0:m<n,\forall(s,t)\in E^1\end{gathered}\tag{34}$$

$$\sum_{j\in V:(i,j)\in E^0}\delta_{ij}^{st}(m,n)-\sum_{j\in V:(j,i)\in E^0}\delta_{ji}^{st}(m,n)=\begin{cases}1-(w_{mn}^{st}+b_{mn}^{st}+w_{nm}^{st}+b_{nm}^{st}) & \text{if}\quad i=s\\ -1+(w_{mn}^{st}+b_{mn}^{st}+w_{nm}^{st}+b_{nm}^{st}) & \text{if}\quad i=t\\ 0 & \text{otherwise}\end{cases}\tag{35}$$

$$\forall i\in V,\forall(s,t)\in E^1,\forall(m,n)\in E^0:m<n$$

$$\sum_{(s,t)\in E^1,(m,n)\in E^0:m<n}(\delta^{st}_{mn}(m,n)+\delta^{st}_{nm}(m,n))=0 \tag{36}$$

Relations (33) to (36) define the new physical paths for each logical link (s,t) allowed to carry BEP traffic when neither its working path nor its backup path are involved into the failure of fiber (m,n). Then the BEP traffic can be sent to either physical path. All this information is kept into the variables $\delta^{st}_{ij}(m,n)$ that are equal to $w^{st}_{ij}+b^{st}_{ij}$ if neither the working nor the backup paths associated to the logical link (s,t) are involved into the failure of fiber (m,n), and to 0 otherwise.

• In each failure state S_{mn}, we use the following to evaluate the new amount of BEP traffic associated with each connection and flowing on each logical link.

$$d^{kh}_{S_{mn}}(BEP)\leq d^{kh}_{S_0}(BEP)$$
$$\forall(k,h)\in\mathcal{C},\forall S_{mn}\in\mathcal{S}\setminus S_0 \tag{37}$$

$$\tau^{st}_{ij}(m,n)\leq B(\sigma^{st}_{ij}(m,n)+\nu^{st}_{ij}(m,n)+\delta^{st}_{ij}(m,n))$$
$$\forall(i,j),(m,n)\in E^0:m<n,\forall(s,t)\in E^1 \tag{38}$$

$$\sum_{j\in V:(i,j)\in E^0}\tau^{st}_{ij}(m,n)-\sum_{j\in V:(j,i)\in E^0}\tau^{st}_{ij}(m,n)=$$
$$\begin{cases} f^{st}_{mn}(BEP) & \text{if} \quad i=s \\ -f^{st}_{mn}(BEP) & \text{if} \quad i=t \\ 0 & \text{otherwise} \end{cases} \tag{39}$$
$$\forall i\in V,\forall(m,n)\in E^0:m<n,\forall(s,t)\in E^1$$

Relation (37) constrains the amount of BEP traffic for each connection; each connection cannot send more BEP traffic during the failure state S_{mn} than the amount it was sending in the no failure state S_0. Relations (38) force the variables $\tau^{st}_{ij}(m,n)$ to be equal to 0 if the physical link (i,j) can not be used to carry the BEP traffic associated to the logical link (s,t) in the failure state (m,n), while relations (39) ensure flow continuity for the BEP traffic.

• The capacity constraints from the physical layer in each failure state S_{mn} are:

$$\sum_{(s,t)\in E^1}(\tau^{st}_{ij}(m,n)+\tau^{st}_{ji}(m,n))\leq(c_{ij}-\sum_{(s,t)\in E^1}(\mu^{st}_{ij}(m,n)+\mu^{st}_{ji}(m,n))-\sum_{(s,t)\in E^1}(\nu^{st}_{ij}(m,n)+\nu^{st}_{ji}(m,n)))\forall(i,j),(m,n)\in E \tag{40}$$

Relation (40) ensures that the total amount of BEP traffic associated with logical links involved in the failure state S_{mn} carried on each physical fiber (i,j) is not larger than the difference between the capacity of the physical fiber and the bandwidth already used by the FP traffic.

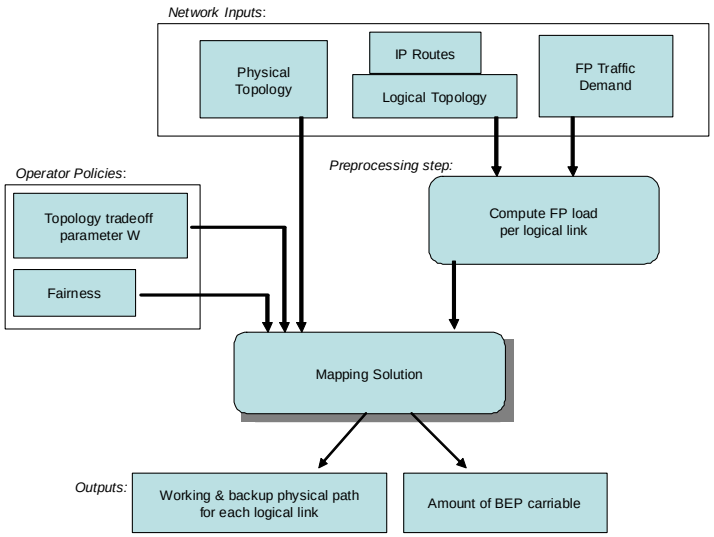

Fig. 1. Block Diagram of Method

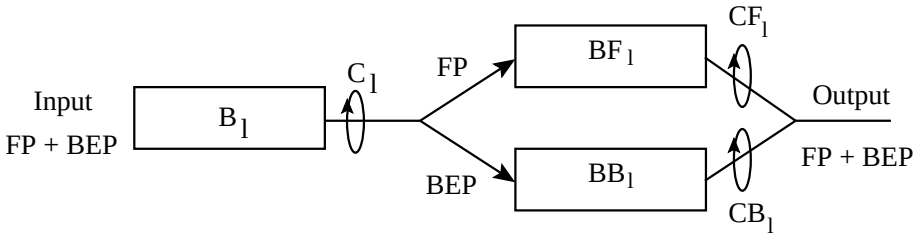

Fig. 2. The scheduler

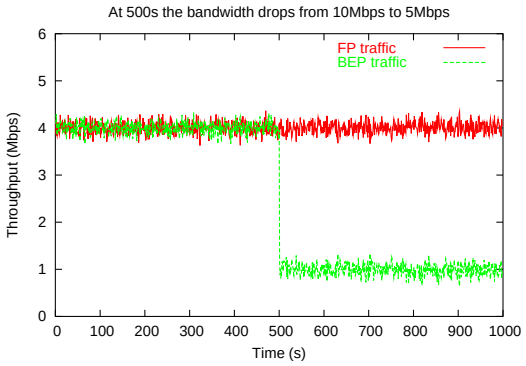

Fig. 3. Throughput for FP and BEP

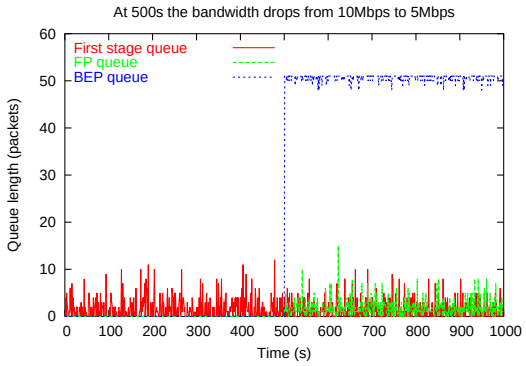

Fig. 4. The occupancy of the three buffers of the scheduler

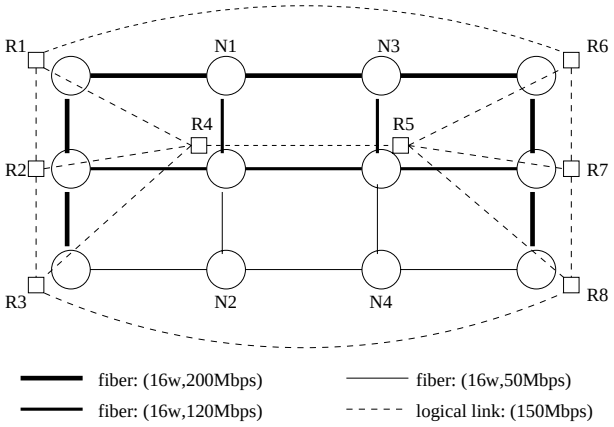

Fig. 5. Medium sized network composed by 12 OXC - 17 WDM fiber at WDM layer and 8 routers - 13 logical links at IP layer.

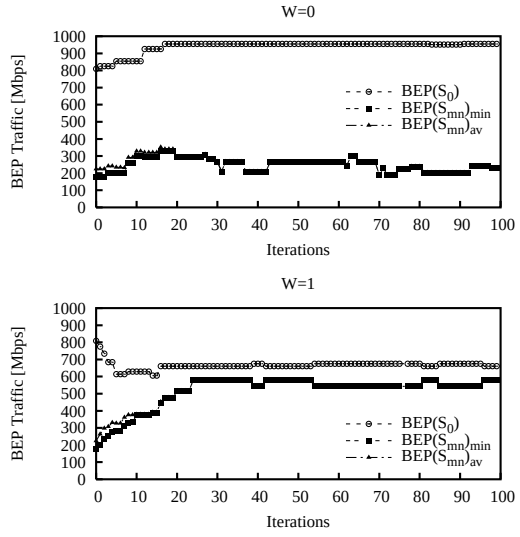

Fig. 6. Tabu Search evolution for $W = 0$ (Optimization in the no-failure state only) and $W = 1$ (Optimization in the single failure state only).No fairness Policies.

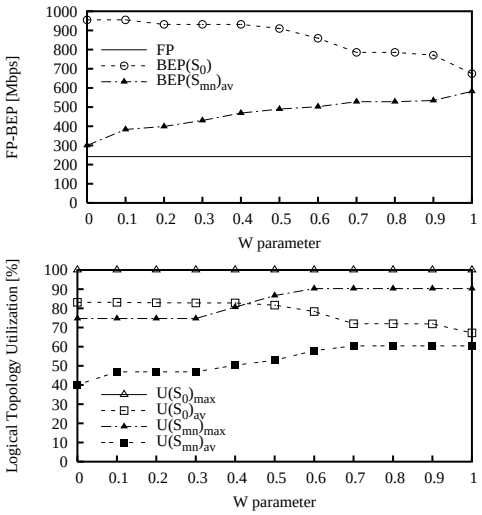

Fig. 7. FP-BEP traffic carried by the network and logical link utilization in all the failure states as a function of the weight W. No fairness Policies.

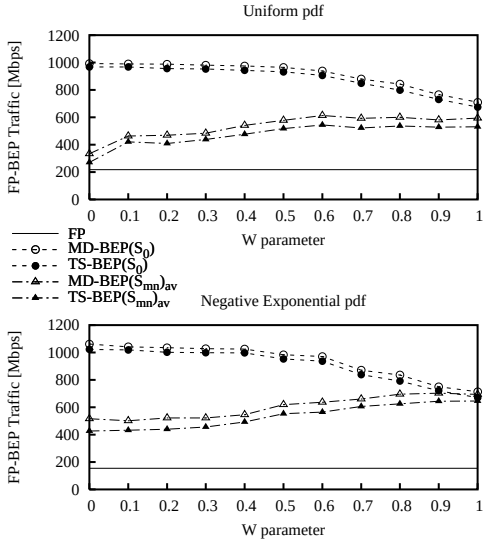

Fig. 8. Comparison between Model and Tabu Search. Two different traffic matrices are analyzed, the first with its entries uniformly distributed, and the second with entries following a negative exponential distribution. No fairness Policies.

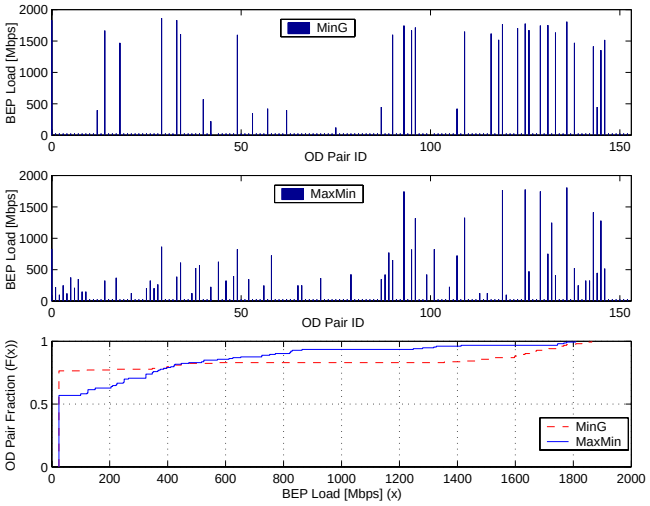

Fig. 9. BEP load distribution among the logical connections for the two fairness policies introduced with a $Z_{min} = 25$ Mbps.

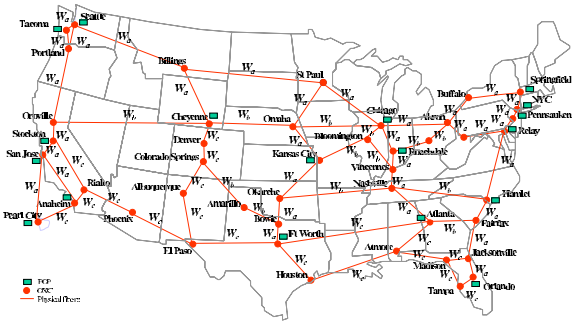

Fig. 10. Sprint WDM Topology: 36 OXC - 55 WDM fibers. Heterogeneous backbone: W_a represent an OC192 system equipped with 40 channels at 10 Gbps, W_b represent an OC48 system with 40 channels at 2.44 Gbps and W_c an OC12 system with 40 channels at 622 Mbps.

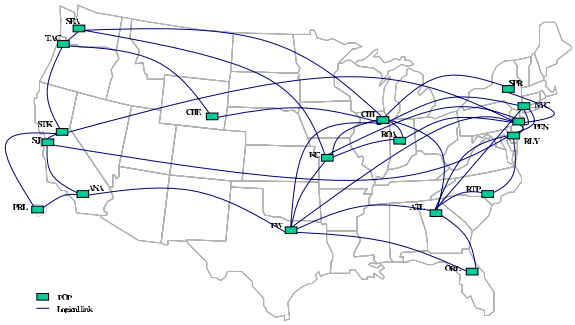

Fig. 11. Sprint Logical Topology: 18 IP PoPs - 36 bidirectional logical links. The line card speed limit is set to 2.4 Gbps for each logical link.

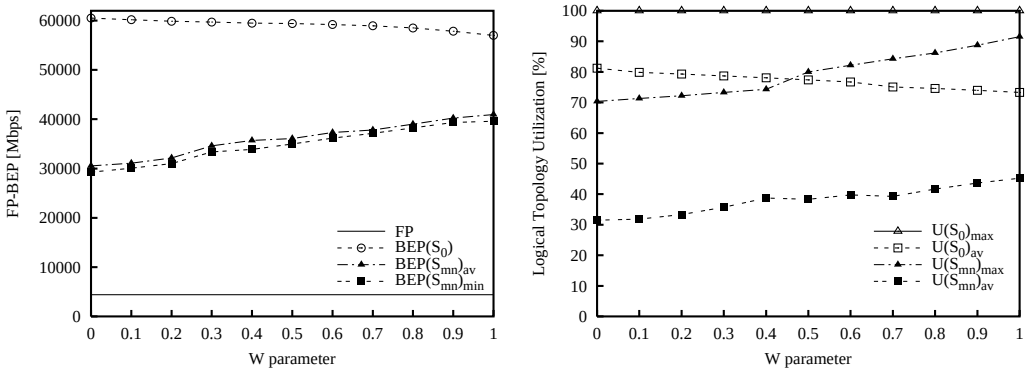

Fig. 12. Sprint backbone results for a uniform traffic matrix.

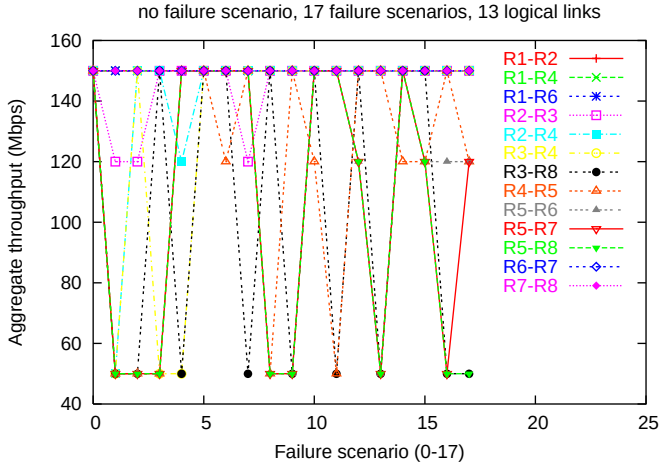

Fig. 13. Bandwidth of each logical link (13 in total) in the normal operation state (failure id 0) and for any physical link failures (failure id from 1 to 17).

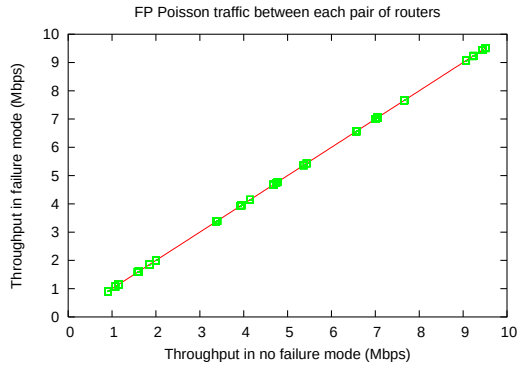

Fig. 14. Throughtput for FP traffic: failure mode versus no failure mode.

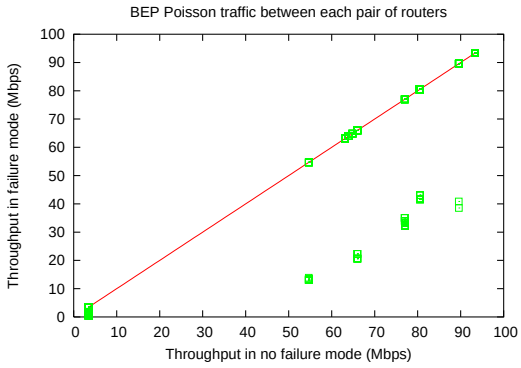

Fig. 15. Throughtput for BEP traffic: failure mode versus no failure mode.

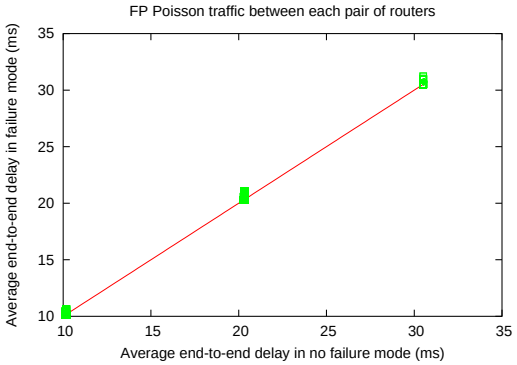

Fig. 16. End-to-End Delay for FP traffic: failure mode versus no failure mode.

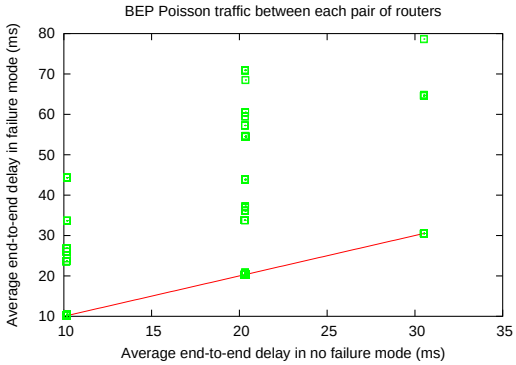

Fig. 17. End-to-End Delay for BEP traffic: failure mode versus no failure mode.

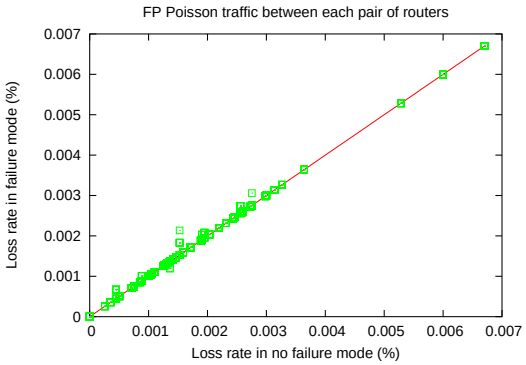

Fig. 18. Losses for FP traffic: failure mode versus no failure mode.

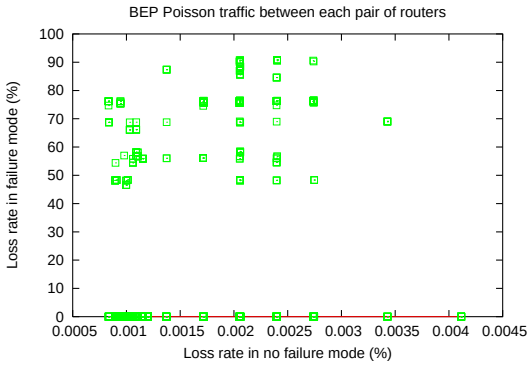

Fig. 19. Losses for BEP traffic: failure mode versus no failure mode.

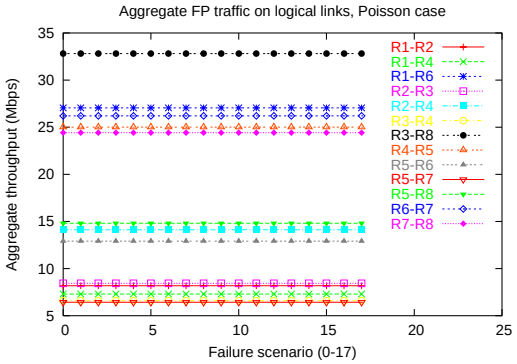

Fig. 20. Average throughput for FP traffic for each failure scenario.

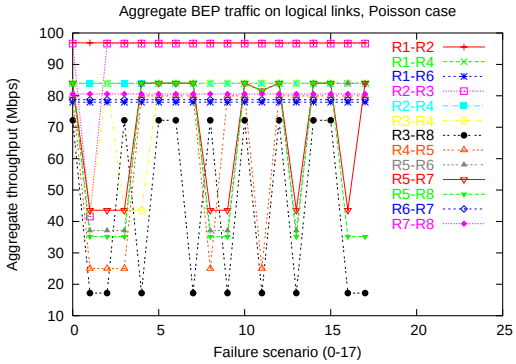

Fig. 21. Average throughput for BEP traffic for each failure scenario.